UNITED STATES DISTRICT COURT

for the

Northern District of Texas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Devices seized from James G. Smith currently located at the US Naval Criminal Investigative Service office at 1701 E. Lamar Blvd, Ste 292, Arlington, Texas

Case No. 4:18-MJ- 265

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Devices seized from James G. Smith currently located at the US Naval Criminal Investigative Service office at 1701 E. Lamar Blvd, Ste 292, Arlington, Texasas described in Attachment A.

located in the Northern District of Texas, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2242(b), 1470, 2252	Attempted Coercion or Enticement, Attempted Transfer of Obscene Materials to a Minor, Possession and Receipt of Child Pornography

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Michael Elkheir, NCIS

Printed name and title

Sworn to before me and signed in my presence.

Date: 4/23/18

Judge's signature

City and state: Fort Worth, Texas

United States Magistrate Judge Jeffrey L. Cureton

Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Special Agent, Michael Elkheir, of the United States Naval Criminal Investigative Service, being duly sworn under oath, do hereby depose and state:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the U.S. Naval Criminal Investigative Service (NCIS), assigned to the Dallas, TX resident agency since September 2015. As such, I am trained as a federal law enforcement officer responsible for conducting criminal investigations of violations of federal law, with a focus on cases having a Department of Defense nexus. As an NCIS Special Agent, I am also authorized to investigate crimes involving the sexual exploitation of children pursuant to Title 18, United States Code, Sections 2422 and 2252. Section 2422 (b) makes it a federal offense to use the mail or any facility or means of interstate commerce, including by a computer or cellular phone, or within the special maritime and territorial jurisdiction of the United States, to knowingly persuade, induce, entice, or coerce any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so.

3. As part of my duties as an NCIS Special Agent, I have gained experience conducting criminal investigations involving child exploitation and child enticement. I am a member of the Internet Crimes Against children (ICAC) Task Force and am responsible for investigating the sexual exploitation of children. I have received training in the area of child exploitation, and as part of my duties, I have conducted investigations involving online solicitation and enticement of minors, including those involving real children and those in which I posed as a child online in proactive investigations. I have also participated in trainings involving the investigation of online solicitation and federal enticement cases, in which computers and other electronic media are used as the means for persuading, inducing, and/or enticing minors to engage in unlawful sexual activity, in violation of 18 U.S.C. § 2422(b) and the transferring of obscene material to minors in violation of 18 U.S.C. § 1470.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

5. The first device to be seized and searched is a Samsung Galaxy J7 Prime cellular phone, serial number unknown, but discovered on the person of **James Gabriel Smith II**, at the time of his arrest on April 18, 2017, in Fort Worth, Texas. The second device to be seized and searched is a Lenovo Ideapad 320 laptop computer, Serial Number PFOR1PJY, seized from Smith's vehicle on April 18, 2018 in Fort Worth, Texas.

6. Both devices are presently located at the U.S. Naval Criminal Investigative Service, 1701 E. Lamar Blvd, STE 292, Arlington, Texas 76011, located within the Northern District of Texas. The applied-for warrant would authorize the seizure and subsequent forensic examination of both devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. On February 6, 2018, your Affiant observed an advertisement posted to an Internet message board website servicing the Dallas - Fort Worth, Texas area. The title of the advertisement read, "Seeking A Relationship With Like Minded Sexual Freak!!! (Saginaw, TX)." The advertisement appeared in a section of the Internet message board that is commonly used to solicit sexual activity. The content of the advertisement included the following statements:

"No matter how many guys, girls, cousins, uncles, etc you've fucked, its fine with me. 20 to 500, its fine. ... No more hiding who you are. No more hiding your sexual past, present, or future. No more hiding your deepest, darkest desires and fantasies. A little about me: I'm a 14 year navy vet. Been out for 3 years. ... I'd like to be in a loving relationship with a women, just as sexual and perverted (504) as me. But I'm also very loving, passionate, and considerate. I love the normal relationship stuff as well. ... About you: You should be age 50 or younger. AGE and RACE is not an issue. Long, straight black/dark brown hair is preferred, but certainly 9308 not a deal breaker!!!! Slim to average body type. A few curves are fine as well. If this sounds like you, my Kik is: airframer_73. Shoot me a message."

8. Based on my prior investigative experience, I know this particular message board has been used in the past by adults to solicit sex from minors within the Northern District of Texas.

I am also aware that the operators of the Internet message board website expressly prohibit any advertisements soliciting sexual activity from minors. To avoid blatantly violating posting restrictions set by the Internet message board website, individuals attempting to entice minors to engage in sexual activity often use key terms or phrases to indicate that they are seeking a sexual partner under the age of eighteen. Examples of such key words and phrases previously identified and known to law enforcement include terms such as son, daughter, niece, nephew, or younger. Based on my previous experience, the reference that age did not matter could be indicative of a person soliciting a sexual encounter with a young female, potentially under the age of 18.

9. On February 7, 2018, your Affiant, posing as a minor female, e-mailed the message board poster of the previously mentioned advertisement. In the e-mail the minor female, (hereafter, "Aleah,") stated, "Hey saw ur post and wanted to give u props,,,im wayyy to young buy still wanted to say hi :) byeeee."

10. Shortly after sending that message, **Smith** replied, "Well, thank you!!! How do you know that you're too young?" Aleah then replied that she was 13 years old, and **Smith** told her to communicate with him via Kik. **Smith** also provided the email address guy4you2017@gmail.com and the telephone number [redacted]-9308, and stated, "we have to be careful. Lol. But yeah, let's talk baby girl."

11. During their initial email communications, **Smith** sent Aleah a copy of his driver's license and asked her to delete the photo after she saw it. He also asked for a photograph of Aleah, stating the following:

> "Idk how much experience u have, but u've obvisouly seen my pics and liked what u saw!! Dirty girl!! And I DO mean that as a compliment!!! Very hot!!!! I like that.....A LOT!!!! But I'd love to see what u look like so that I can see who I'll be kissing and rubbing my hands all over u. And feeling ever inch of u and eventually move my hands to ur tits, and little pussy. Maybe even lick it and make u feel good. But of course we don't have to move that fast. We can go as slow as u want. Cuz like I said, Idk how much experience u have yet. But no experience is fine too. I can teach u :)"

12. **Smith** also told Aleah:

> "I know u need to trust me 1st. That's why we can go at ur pace. As slow as u need. For me, this is all about u!!!!! So I WANT u to trust me before anything. Take as long as u need. I will never rush u!!!!! Trust is earned, so take as long as u need. As for ur experience, I already assumed that u didn't have any, so I don't mind. I don't expect u to know how to do things, like suck dick, or anything else ur dirty little mind can come up with. So don't worry about that. It's ok. :)) And obviously I don't want to get in trouble. Lol That would be really bad for me. So obviously u can't tell anyone we're talking."

13. On February 19, 2019, Aleah told **Smith** her aunt was going out of town; and the two discussed over text messages the possibility of meeting. **Smith** stated he was interested in coming over on February 22, 2018, but that he was scared because he had heard about men chatting with police officers instead of minor females and getting arrested when they showed up at the "girl's" house. **Smith** requested Aleah prove that she was in fact a real minor; at that point, Aleah told **Smith** that he was scaring her and called off the meeting. **Smith** apologized for overreacting and doubting that she was a real minor. Communications between the two ceased for approximately three weeks.

14. On March 20, 2018, **Smith** contacted Aleah via text message and told her he missed her. **Smith** also sent approximately 15 images of his penis in erect and flaccid states through texts.

In the weeks that followed, **Smith** told Aleah that he had previously dated a 17-year-old female, with whom he had had a long-term relationship. **Smith** also continued to engage in sexually explicit conversations with Aleah via text messaging. On April 12, 2018, while texting with Aleah, **Smith** stated that he sees her as a "beautiful, sexy goddess" and later that day asked her to "reach down and put ur hand in ur pants, and feel ur pussy, just for a second." **Smith** sent additional pictures of his penis, telling Aleah on April 16, 2018, to "keep fucking yourself with ur fingers."

15. Also during their text communications, **Smith** asked Aleah when her aunt was going out of town again. On April 17, 2018, Aleah mentioned that her aunt was going out of town. On April 18, 2018, **Smith** offered to come over to her home, telling her that he would only engage in whatever sexual activity that Aleah was comfortable with. Aleah provided **Smith** with an address to an apartment located in Fort Worth, Texas. When **Smith** arrived at the location and knocked on the apartment door, he was intercepted by NCIS agents. At the time of his arrest, **Smith** was in possession of a condom and the Samsung Galaxy J7 Prime cell phone. On the home screen, a push notification showing Aleah's text was visible. The cell phone was seized as evidence.

16. Shortly after **Smith** was taken into custody, NCIS agents conducted a search of his vehicle. During that search, agents recovered a silver in color Lenovo Ideapad 320, SN#PFOR1PJY.

17. That same evening, your Affiant advised **Smith** of his *Miranda* warnings, which he acknowledged that he understood, and agreed to speak to agents. **Smith** admitted that he traveled to Aleah's apartment and that he wanted to have sex with her.

Smith also said that he was currently speaking with another girl who is 16 years of age and that he had received a topless photo of the minor. **Smith** was asked if he had any nude photographs of underage girls, and he stated that on both his laptop and cell phone he had numerous sexually explicit photos and videos of his ex-girlfriend. Although Smith indicated that his girlfriend was 18 years of age at the time they were taken, in light of Smith's repeated requests for nude images of the purported minor, his representation to the minor that he had been involved in a relationship with a 17-year old, and his possession of a topless image of a minor, there is probable cause to believe that sexually explicit images and videos of a minor or minors will be located on Smith's laptop computer.

18. Further, your affiant knows, based on training and experience, that digital photographs taken by means of cellular telephones, digital cameras, and video cameras can be transferred to and stored in other digital storage media including but not limited to laptop computers. I am also aware that cell phones are frequently backed up to laptop computers. In the commission of this offense, Smith utilized three Internet based communication services, a web-site (Craigslist), email service (Gmail), and an instant messaging service (Kik). **Smith** was found in possession of two devices that are capable of accessing Internet based services, a Lenovo Ideapad 320 laptop and a Samsung Galaxy J7 Prime smartphone.

19. Affiant knows from his experience and conversations with fellow law enforcement officers who investigate Cyber-crime, that there is a fair probability that an offender with access to more than one computer, to include smartphones, will utilize multiple computers in the commission of an Internet based offense.

20. Affiant knows that offenders will either directly communicate with their victims on multiple computer devices or will restrict their direct communication to one device while creating, managing, and exercising control of the accounts used to communicate with the victim from a second device. The exercise of control over the account may include either accessing the account itself or by accessing another account which is set as the "backup", "secondary", or "recovery" account.

21. In cases where files are exchanged between the offender and victim, such as images and videos, Affiant knows that offenders will intentionally or accidently store said files to cloud based storage services, such as Google Drive and Dropbox, which are synced (i.e. transferred) to or are otherwise accessible from the offender's other computer device(s).

TECHNICAL TERMS

22. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone.

In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every phone or computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that phone or computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses.

d. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

23. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at https://www.samsung.com/us/mobile/phones/all-other-phones/samsung-galaxy-j7-16gb-t-mobile-white-sm-j700tzwatmb/, I know that **Smith's** cell phone has capabilities that

allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

24. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the Device. This information can sometimes be recovered with forensics tools.

25. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. Based on my training and experience, I am aware that the search of computers often requires agents to seize most of the computer items (e.g., hardware, software and instructions) to be processed later by a qualified computer expert in a laboratory or other controlled environment. That is essential to the search for electronic evidence because of the following facts:

26. Computer storage devices, like hard drives, diskettes, tapes, or laser disks, store the equivalent of thousands of pages of information. When a user wants to conceal electronic evidence of a crime, he or she may store it in random order with deceptive file names. This requires searching authorities to examine all of the stored data to determine whether it is included within the scope of the warrant. This process can take weeks or months, depending on the volume of the stored data, and it would be impractical to attempt this kind of data search on-site;

27. Searching computer systems for criminal evidence is a highly technical process that requires advanced training and a properly controlled environment. The vast array of computer hardware and software available today requires even computer experts to specialize in specific systems and applications. It is difficult to know prior to a search which expert should analyze the system and its data.

The search of a computer system can be equated to a scientific procedure, which is designed to protect the integrity of the evidence while recovering hidden, erased, compressed, password-protected, and other encrypted files. Because computer evidence is extremely vulnerable to tampering and destruction, both from external sources and from code embedded in the system as a "booby-trap," the controlled environment of a laboratory is essential to its complete and accurate analysis;

a. In order to fully retrieve data from a computer system, an analyst needs all magnetic storage devices, as well as the central processing unit (CPU);

b. Searching computerized information for evidence or instrumentalities of a crime often requires the seizure of the entire computer's input/output periphery devices, including related documentation, passwords and security devices, so that a qualified examiner can accurately retrieve the system's data in a controlled environment. Peripheral devices, which allow users to enter and retrieve data from stored devices, vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system; therefore, it is important that the analyst be able to properly retrieve the evidence sought.

28. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

29. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

30. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of such criminal offenses may be located in the devices described in Attachment A, in violation of 18 U.S.C. §§ 1470, 2422(b) and 2252.

31. I, therefore, respectfully request that the attached warrant be issued authorizing a search for the items listed in Attachment B.

Michael Elkheir, Special Agent
Naval Criminal Investigative Service

Subscribed and sworn to before me on this the 23rd day of April, 2018, at 2:07 p.m. in Fort Worth, Texas

JEFFREY L. CURETON
United States Magistrate Judge

ATTACHMENT A

The property to be seized and searched is a Samsung Galaxy J7 Prime cellular phone, serial number unknown, but discovered on or about the person of **James Gabriel Smith II**, at his time of arrest April 18, 2017, in Fort Worth, TX, and place into evidence at the at the U.S. Naval Criminal Investigative Service, which is currently located at 1701 E. Lamar Blvd STE 292, Arlington, Texas 76011, hereinafter the "Device." The Device is currently located at the NCIS Resident Agency Dallas, located at 1701 E. Lamar Blvd STE 292, Arlington, Texas 76011.

Also to be searched is described as a Lenovo Ideapad 320 laptop computer, Serial Number PFOR1PJY, seized from Smith's vehicle on April 18, 2018 in Fort Worth, Texas. The device is presently located at the U.S. Naval Criminal Investigative Service, which is currently located at 1701 E. Lamar Blvd STE 292, Arlington, Texas 76011, located within the Northern District of Texas.

This warrant authorizes the forensic examination of the cell phone and laptop computer for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the devices described in Attachment A that relate to violations of 18 U.S.C. § 1470 [Attempted Transfer of Obscene Material to a Minor], 18 U.S.C. § 2422(b) [Attempted Coercion or Enticement], and 18 U.S.C. § 2252 [Receipt and Possession of Child Pornography] and involve **James Gabriel Smith II**, including:

   a. All stored contacts, address books, calendar appointments;

   b. Images or video used to promote or further the trafficking of children.

   c. Any locations marked by Global Positioning Satellites (GPS) that are associated with the attempted enticement of minors and or attempted transfer of obscene materials to a minor;

   d. Any applications and its contents, such as Kik and Skype, that may have been used to communicate with minors for the purpose of committing violations involving the sexual exploitation of minors.

2. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

   a. evidence of software that would allow others to control the devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

   b. evidence of the lack of such malicious software;

c. evidence indicating how and when the devices were accessed or used to determine the chronological context of each device's access, use, and events relating to crime under investigation and to the computer user;

d. evidence indicating the device user's state of mind as it relates to the crime under investigation;

3. Records evidencing the use of the Internet to communicate with Google servers and or Craigslist servers, or any other Internet servers promoting the business of enticement, prostitution or trafficking of minors including:

a. records of Internet Protocol addresses used;

b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.